## Amendments to the Claims

1. (Currently Amended) A method of enabling a proxy client in a secured network to access a target service on behalf of a user, comprising the steps of:

registering proxy authorization information regarding the user with a trusted security server, the proxy authorization information identifying the proxy client and an extent of proxy authorization, the extent of proxy authorization comprising a restriction on a range of target services that the proxy client may access on behalf of the user;

submitting, by the proxy client, a proxy request to the trusted security server requesting access to the target service on behalf of the user;

comparing, by the trusted security server, the proxy request with the proxy authorization information of the user to determine whether to grant the proxy request;

issuing, by the trusted security server, a data structure containing authentication data recognizable by the target service for authenticating the proxy client for accessing the target service on behalf of the user~~; and~~

~~accessing, by the proxy client, the target service, the access being in a batch mode without user intervention~~.

2. (Original) A method as in claim 1, wherein the data structure is a ticket containing a session key for use in a session formed between the proxy client and the target service.

3. (Original) A method as in claim 1, wherein the ticket is encrypted with a secret key shared by the target service and the trusted security server.

4. (Original) A method as in claim 1, wherein the step of comparing determines whether a proxy duration specified by the proxy authorization information has expired.

5. (Original) A method as in claim 1, wherein the step of submitting the request includes transmitting a ticket for authenticating the proxy client to the trusted security server.

6. (Previously Presented) A computer-readable medium having computer-executable instructions for a trusted security server to perform the steps:

storing proxy authorization information from a user for authorizing a proxy client to act as a proxy of the user;

receiving a proxy request from the proxy client to access a target service on behalf of the user;

determining, based on the proxy authorization information of the user, whether to grant the proxy request;

constructing a data structure containing authentication data recognizable by the target service for authenticating the proxy client for accessing the target service on behalf of the user.

7. (Original) A computer-readable medium as in claim 6, having further computer-executable instructions for performing the step of authenticating the user based on a password of the user before storing the proxy authorization information.

8. (Original) A computer-readable medium as in claim 6, wherein the step of receiving the proxy request includes authenticating the proxy client based on a ticket issued to the proxy client for communicating with the trusted security server.

9. (Original) A computer-readable medium as in claim 6, having further computer-executable instructions for performing the step of sending the data structure to the proxy client for presenting to the target service for authentication of the proxy client.

10. (Original) A computer-readable medium as in claim 6, wherein the data structure is encrypted with a key shared by the target service and the trusted security server.

11-17. (Cancelled)